

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-25051

(43) 公開日 平成11年(1999) 1月29日

(51) Int.Cl. ⁶	識別記号	F I
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00 3 3 0 B
1/00	3 7 0	1/00 3 7 0 E

審査請求 未請求 請求項の数10 O L (全 9 頁)

(21) 出願番号 特願平9-183433

(22) 出願日 平成9年(1997) 7月9日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 横沢 達

神奈川県横浜市戸塚区吉田町292番地株式

会社日立製作所マルチメディアシステム開
発本部内

(72) 発明者 安達 誠

神奈川県横浜市戸塚区吉田町292番地株式

会社日立製作所マルチメディアシステム開
発本部内

(74) 代理人 弁理士 小川 勝男

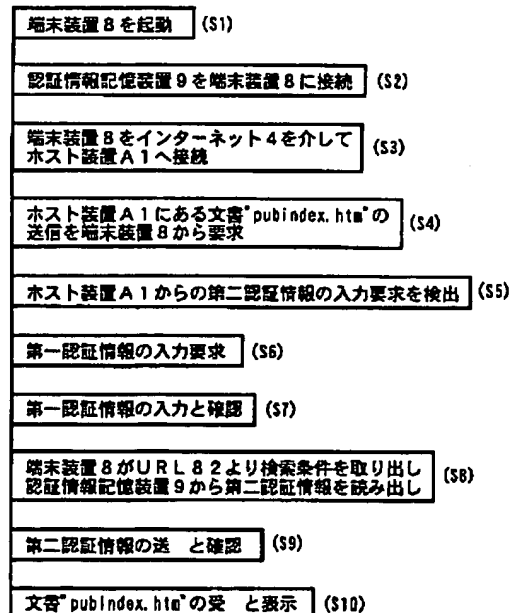
(54) 【発明の名称】 情報システム

(57) 【要約】

【課題】 端末装置を複数箇所のホスト装置に接続するときに、複数の異なる認証情報が必要になる場合があり、これでは利用者は必要な認証情報をすべて覚えておく必要があるため非常に煩わしい。

【解決手段】 端末装置にホスト装置へ送信する複数の認証情報を記憶し、またこの認証情報を読み出す為にこれらとは別の認証情報を必要とし、またこの別に用意した認証情報を確認するための機能を備えた情報システム。

図 6



【特許請求の範囲】

【請求項 1】各種情報を蓄積し、該情報を端末装置により利用者が取り出し可能で、該利用者が前記情報の取り出しを行うときに、利用者が正規の登録者であることを確認するための認証情報を利用者に要求する機能を有するホスト装置と、

該ホスト装置と接続してデータの送受信が可能で、前記各種情報を取り込み、これを利用者に提示する機能と、利用者からの入力を受ける機能を有する前記端末装置と、

からなる情報システムにおいて、

各種のデータを記憶し、前記端末装置によって該データの読書きをすることが可能で、かつ、該データの読書きする前に、これを許可するための第一認証情報を記憶し、さらに該許可処理を行う機能を有する認証情報記憶装置を備え、

該認証情報記憶装置が前記ホスト装置で必要となる認証情報を第二認証情報として記憶し、さらに該第二認証情報を選択的に読書きできる機能を前記認証方法記憶装置または前記端末装置に備え、

第二認証情報を複数種類必要とする場合でも、利用者がそれぞれの認証情報を覚えなくとも、唯一前記第一認証情報だけを覚えるだけで簡単な選択で必要な第二認証情報を読み出して、前記ホスト装置への接続に必要な確認処理を完了できるようにしたことを特徴とする情報システム。

【請求項 2】請求項 1 において、前記ホスト装置と前記端末装置がプロトコルによって情報の送受信を行う機能を備え、

前記端末装置が該プロトコルによって前記ホスト装置との接続に確認処理が必要であることを検出する機能と、該検出結果を契機として該端末装置が前記第二認証情報を前記認証情報記憶装置より読み出して前記ホスト装置へ送信する機能、および予め前記認証情報記憶装置への前記第一認証情報による確認手続きを完了しておく機能を備え、

前記ホスト装置より前記第二認証情報を要求されたときに、その度に利用者が前記第一認証情報の入力を行う必要がないようにしたことを特徴とする情報システム。

【請求項 3】請求項 2 において、ホスト装置と端末装置が TCP/IP によって接続され、前記第二認証情報を前記認証情報記憶装置から選択的に読み出すための条件情報として、IP アドレスを用いることを特徴とする情報システム。

【請求項 4】請求項 1 または請求項 2 において、前記第二認証情報を認証情報記憶装置から選択的に読み出すための条件情報が、URL (Uniform Resource Locator) を用いることを特徴とする情報システム。

【請求項 5】請求項 2 において、予め第一認証情報によって行った前記認証情報記憶装置への読み書きが出来る

有効な期間が、前記端末装置と前記ホスト装置との接続を切断する時に終了することを特徴とする情報システム。

【請求項 6】請求項 2 において、予め第一認証情報によって行った前記認証情報記憶装置への読み書きが出来る有効な期間が、前記端末装置または認証情報記憶装置に予め設定された期間を経過すると終了することを特徴とする情報システム。

【請求項 7】請求項 2 において、前記端末装置が予め設定された時間で自動的に端末機能を停止する機能を備える場合、予め第一認証情報によって行った前記認証情報記憶装置への読み書きが出来る有効な期間が、該端末機能の停止で終了することを特徴とする情報システム。

【請求項 8】請求項 1 において、前記認証情報記憶装置が利用者の操作で前記端末装置から分離して携帯出来ることを特徴とする情報システム。

【請求項 9】請求項 2 において、前記認証情報記憶装置が利用者の操作で前記端末装置から分離して携帯でき、予め第一認証情報によって行った前記認証情報記憶装置への読み書きが出来る有効な期間が、前記認証情報記憶装置を前記端末装置から分離した時に終了することを特徴とする情報システム。

【請求項 10】請求項 1 において、前記認証情報記憶装置が記憶したデータの読み書きを自由に行うことが可能で、前記端末装置が利用者が暗記する暗証情報を鍵データとしてデータの暗号化と復号化を行う機能を備え、前記第二認証情報を暗号化して認証情報記憶装置に記憶させ、必要に応じて前記暗証情報によって前記記憶させた暗号情報を復号化して第二認証情報を読み出すようにし、第二認証情報が漏洩するのを防止すると共に、唯一前記暗証情報だけを覚えるだけで簡単な選択で必要な第二認証情報を読み出して、前記ホスト装置への接続に必要な確認処理を完了できるようにしたことを特徴とする情報システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、特定情報あるいは特定ホスト装置に対する利用者認証に係わり、特に利用者認証情報が対象情報毎あるいはホスト装置毎に異なる場合に、利用者がこれら複数の認証情報を覚える必要がない情報システムに関する。

【0002】

【従来の技術】近年、インターネット上で急速に広がっている World Wide Web (欧州核物理学研究所で開発されたドキュメントシステムで以下、WWW) に代表されるように、ネットワーク上の情報提供システム (例えば WWW サーバ) では特定のホスト装置への接続のみならず、そのホスト装置の認証が終了した後も、さらにその中にある特定の情報に対しても利用者の認証を求められる場合がある。

【0003】この場合、利用者はその都度予め取得した認証情報をホスト装置に送信する必要がある。

【0004】

【発明が解決しようとする課題】しかしながらこれら認証情報は、ホスト装置の管理者の都合で決定されたものを利用する場合があり、このような時は認証情報がホスト装置毎または情報毎に異なるのが通例である。しかし、これでは利用者は必要な認証情報をすべて覚えていなければならない、非常に煩わしい。

【0005】しかも、認証情報は利用者本人以外へ漏れることが無いように扱う必要がある、メモ書き等を残すことは好ましくない。

【0006】本発明の目的は上記の点に鑑みてなされたもので、その目的は、利用者は唯一、一個の認証情報を入力するだけで、その後はホスト装置または情報への認証処理が簡単に行えるようにすることにある。

【0007】

【課題を解決するための手段】上記目的を達成する本発明の要旨は、ホスト装置へ送信する複数の認証情報を記憶し、またこの認証情報を読み出す為に送信するものとは別に認証情報を必要とし、さらにこの別に用意した認証情報を確認するための機能を有する認証情報記憶装置と、認証情報記憶装置への認証情報の書き込み、あるいは同装置から認証情報を読み出す機能を有する端末装置を備える。

【0008】

【発明の実施の形態】以下、本発明の詳細を図示した各実施例によって説明する。

【0009】【第一実施例】図1は、本発明の第一実施例に係わる情報システム概念図である。本実施例は、プロトコルを使い、インターネット4上のWWWサーバから利用者10が必要とする情報を取り寄せる例を示したものである。

【0010】図1において、1、2および3は情報を蓄積しインターネット4に接続されたWWWに対応したホスト装置A、BおよびCで、これらは後述する端末装置8と接続するときに、利用者10が正規の利用者であることを確認するために、第二認証情報を要求する。4はホスト装置間または利用者10との間で情報の送受信を可能にするネットワークでインターネット、5は利用者10とインターネット4の仲介を契約によって行うインターネットプロバイダである。また、6は利用者10とインターネットプロバイダ5を接続する公衆回線網、7は公衆回線網6から端末装置8までを接続する公衆回線。

【0011】8は利用者10がWWWから情報を取り出すために使用する端末装置で、後述するWWWを利用するためのブラウザソフト12を搭載しており、情報の表示と利用者からの入力が行える機能を持ち、さらに後述する認証情報記憶装置9に記憶されたデータの読み書き

が可能である。9は端末装置8をホスト装置に接続するために要求される第二認証情報と、この第二認証情報が他に漏れないように保護するための第一認証情報を記憶し、また端末装置8で第二認証情報の読み書きを行う時は、必ず第一認証情報により予め認証処理を行う機能を内蔵しており、さらに図5で後述する検索条件により第二認証情報を選択的に読み書きする機能も備えた認証情報記憶装置である。

【0012】10は本システムの利用者、11はホスト装置と端末装置8の間のインターネット4および公衆回線7上で、情報のデータを乗せて流れるプロトコルのパケットである。

【0013】12はプロトコルによってホスト装置と通信を行い、ホスト装置に格納された文書を端末装置8の表示機能により利用者10に提示するソフトウェアでブラウザソフトである。ブラウザソフト12は利用者10から入力されたホスト装置や文書名を表わす情報に基づいてインターネット4にアクセスし、ホスト装置より認証情報が要求されたことを検出して、認証情報を認証情報記憶手段9より読み出して送信する機能と、未だ第一認証情報の認証が完了していないために第二認証情報を読み出せない場合には、第一認証情報の入力を利用者10に要求する機能を備える。

【0014】図2は本実施例においてホスト装置A1、ホスト装置B2およびホスト装置C3から情報を取得するために必要となる「利用者ID」とそれぞれに対応した「認証情報」、および各ホストを表わす「サーバ名」の例を示している。ここでは、ホスト装置B2とホスト装置C3の認証情報は同じであるが、それ以外は全て異なるものが必要であり、これらを一通り覚えるのは面倒である。

【0015】図3は本実施例において、ブラウザソフト12が利用者10に対して認証情報記憶装置9の読み書きを可能にするための第一認証情報を要求している様子を示しており、81はその第一認証情報を入力する認証情報入力欄である。

【0016】図4は本実施例において、利用者10が端末装置8をホスト装置A1に接続したときの端末装置8の画面の例で、82はインターネット4上で特定のホスト装置を指定するための記述手段であるUniform Resource Locator（以下URL）であり、“//www.earth.co.jp”はサーバ名で、“/pubindex.htm”はホスト装置から取り寄せる文書名を表わしている。

【0017】本実施例では、この“pubindex.htm”という文書の取得に認証情報が要求されるとする。また、83は前述の文書を参照するために必要な利用者名を入力する利用者ID入力欄で、84は同じく第二認証情報を入力するための認証情報入力欄である。

【0018】図5は本実施例において、認証情報記憶装置9の中に各認証情報を記憶するときのデータ構造の例

を示したもので、91は認証情報記憶装置9の利用者10を確認するための第一認証情報であり、これが認証されないといこれに続く他のデータへの読み書きが認証情報記憶装置9自身によって禁止される。

【0019】また92は図2に示したホスト装置へ送信する第二認証情報で、93はこの第二認証情報を簡単に選択できるようにするための検索条件であり、本実施例ではサーバ名と文書名を利用している。さらに、94は利用者ID、95は認証情報で、これらは第二認証情報92の要素データである。なお、認証情報記憶装置9の中で第二認証情報92と検索条件93は一組にしてレコードという簡単に扱われ、ブラウザソフト12によって読み書きされる。

【0020】図6は本実施例において、ホスト装置A1より文書“pubindex.htm”を端末装置8に取り寄せるときの流れを示した図であり、処理はS1からS10へと進む。

【0021】本実施例の動作を図1～図6を用いて説明する。ここで、利用者10はすでに図2に示すようにインターネット4上のホスト装置A1、ホスト装置B2、およびホスト装置C3を利用するための、第二認証情報92（利用者ID94と認証情報95）を取得しており、これらの情報は図5に示すように、認証情報記憶装置9に検索条件93と共に記憶されている。そして、これから利用者10は公衆回線6を介して、インターネット4に接続されたホスト装置A1から情報を取り寄せようとしているとする。

【0022】まず、利用者10は図6に示すように、端末装置8を起動（S1）し、次で認証情報記憶装置9を端末装置8に接続する（S2）。

【0023】次に、利用者10は図1にあるようにブラウザソフト12を使って、端末装置8を公衆回線7から公衆回線網6を通してインターネットプロバイダ5に接続し、さらに図4のようにURL82にホスト装置A1のサーバ名“//www.earth.co.jp”を指定して、インターネット4を介してホスト装置A1へ接続を行う（S3）。そして、目的の文書名“pubindex.htm”をパケット11に乗せてホスト装置A1へ送信する（S4）。

【0024】ここで、ホスト装置A1は文書“pubindex.htm”に認証確認が設定されていると、このことを端末装置8へ通知し、利用者に対して第二認証情報92の送信を要求する。すると端末装置8のブラウザソフト12はこの要求を検出（S5）して、認証情報記憶装置9から検索条件93を用いて第二認証情報92の取得を試みる。

【0025】しかし、本実施例では図6のS5までの間に未だ第一認証情報91の確認が行われていないため、ブラウザソフト12が認証情報記憶装置9から第二認証情報92を取り出そうとしても、認証情報記憶装置9に

よってその操作が拒否されてしまう。そこで、ブラウザソフト12は図3に示すように、利用者10に対して第一認証情報91の入力を促す（S6）。

【0026】利用者10が認証情報入力欄81に第一認証情報91“Treasure Box”を入力し、「OK」を指示すると、ブラウザソフト12は端末装置8を介して第一認証情報91を認証情報記憶装置9に入力する。第一認証情報91を受け取った認証情報記憶装置9は、これと記憶している第一認証情報が一致するかどうかを確認し、一致した場合には、第二認証情報92の取り出しを許可する（S7）。

【0027】もし、一致しなかった場合には利用者10に対し警告するメッセージの表示や、再入力を促すように動作する。

【0028】S7において確認がされると、次にブラウザソフト12は認証情報記憶装置9に第二認証情報92を検索させるためにURL82に含まれているサーバ名および文書名を渡す。サーバ名と文書名を受け取った認証情報記憶装置9は、図5に示すようにレコード単位で記憶されたデータから検索条件93を順次取り出し、これとサーバ名および文書名を比較して、一致するレコードを探す。

【0029】本実施例では図5で先頭にあるレコードが検索条件93を満たすので、認証情報記憶装置9は同じレコードから検索条件93に続いて記憶されている第二認証情報92（利用者ID94“IslandABC”および認証情報95“173161n64”）を取り出し、これをブラウザソフト12に渡す（S8）。

【0030】ブラウザソフト12はこのようにして第二認証情報92を受け取ると、図4に示した利用者ID入力欄83と、認証情報入力欄84からホスト装置A1に対して第二認証情報92を送信する。第二認証情報92を受信したホスト装置A1は、これを文書“pubindex.htm”に設定されている認証情報と比較し、一致が確認（S9）できると、文書“pubindex.htm”をパケット11に乗せて送信を開始し、ブラウザソフト12はパケット11を順次受信して、端末装置8の画面に文書を表示する（S10）。

【0031】以降、利用者10が新たなURL82を入力し、第二認証情報92が要求される度に、図6に示すS4からS10の処理を繰り返すが、第一認証情報91の確認は既に完了しているので、S6およびS7はスキップされる。

【0032】なお、図6の流れ図では示していないが、もしもS8で検索条件93と一致するレコードが記憶されていないときには、要求された第二認証情報92が記憶されていないことを利用者10に通知する表示と共に、図4の表示で利用者ID入力欄83と認証情報入力欄84が共に空白の表示を行い、そして、ここでもし利用者10が検索条件93に対応する第二認証情報92を

入力すれば、この認証情報は新規の第二認証情報として認証情報記憶装置 9 に検索条件 9 3 と共に記憶され、次回同じ検索条件 9 3 でレコードの検索が行われたときには、自動的に第二認証情報の読み出し処理が行われるようになる。

【0033】また、図 5 で検索条件 9 3 が “www. world-wide.co.jp” のレコードには利用者 ID “Guest” だけが記憶されているが、これはこのホスト装置が認証情報 9 5 を必要としないからである。

【0034】このように処理が行われることにより利用者 1 0 は、一度だけ認証情報記憶装置 9 を利用するための第一認証情報 9 1 を入力しておけば、特定のホスト装置あるいは特定の文書毎に第二認証情報を要求されるような場合、さらにはそのような認証情報の内容がばらばらであるような場合でも、必要とされる第二認証情報が予め認証情報記憶装置 9 に記憶してあれば、利用者 1 0 が暗記している第二認証情報 9 2 を毎回手動で図 4 の利用者 ID 入力欄 8 3 と認証情報入力欄 8 4 に入力しなくても、自動的に第二認証情報 9 2 が送信されるので、入力の間違いがなくなるだけでなく、複数ある認証情報をまとめて一個の認証情報を覚えておくだけで利用できるため非常に使い勝手が良い。

【0035】また、認証情報は利用者以外に漏れることがないようにしなければならないが、本実施例では認証情報記憶装置 9 自身に記憶したデータの読書きを制限する機能を備えているので、たとえ端末装置 8 から分離して紛失したような場合でも、第二認証情報 9 2 が他人に漏れる心配が無い。もちろん、認証情報記憶装置 9 が端末装置 8 と一体になっているような場合でもこれらの利点が失われることがないのは明白である。

【0036】さらに、実施例では説明しなかったが、図 6 で S2 を行わなかったときは、端末装置 8 をホスト装置 A 1 に接続し、文書 “pubindex.htm” を指定したときに、認証情報記憶装置 9 が端末装置 8 に接続されていないことをブラウザソフト 1 2 が検出し、利用者 1 0 に対して認証情報記憶装置 9 を端末装置 8 に接続することを促すメッセージを表示する。そして表示にしたがって、利用者 1 0 が認証情報記憶装置 9 を端末装置 8 に接続すると、図 3 に示したように、第一認証情報 9 1 を入力する画面を表示するようになる。

【0037】また、本実施例では検索条件 9 3 として URL 8 2 に含まれるサーバ名や文書名を利用するようにしたが、検索条件にはこれら以外にもホスト装置と端末装置間のデータ送受信を行っているプロトコルに含まれるデータ、例えば IP アドレスも使うことが可能であり、文書名もそのホスト装置が認証を設定可能なテキスト、音声、画像、などファイルさまざまなものが利用できることは容易に想像できる。

【0038】なお、本実施例では第一認証情報が確認されていれば、後は自動的に第二認証情報が読み出される

ようにしたが、もちろん第二認証情報が必要になる毎に第一認証情報の入力を利用者に要求することも可能で、この場合利用者は多少の不便を被るが、第一認証情報が確認済みの状態で端末装置を放置してしまうと、第三者でも容易にホスト装置の利用が可能になるので、これを防止するためには役立つ。

【0039】図 7 は上記に関して、別の実現形態を示すもので、第一認証情報 9 1 の確認が完了した後の認証情報記憶装置 9 への読み書きが出来る有効期間を終了させる方式の例を示したものである。図 7 では、認証情報記憶装置 9 が端末装置 8 と分離可能である場合を想定し、4 種類の条件で上記の有効期間を終了する。

【0040】まず、認証情報記憶装置 9 の読書き有効期間が開始すると、端末装置 8 またはブラウザソフト 1 2 は定期的に図 7 の流れで、(1) 端末装置 8 とホスト装置との接続終了、(2) 予め端末装置 8 がブラウザソフト 1 2 に設定されている期間端末装置 8 が放置された、(3) 認証情報記憶装置 9 の中に独立して設定された期間が経過した、(4) 認証情報記憶装置 9 が端末装置 8 から分離された、と云う以上の条件を順次確認し、いずれかに該当したときに認証情報の読書き有効期間を終了させ、再び第二認証情報 9 2 が必要なときは第一認証情報の確認からやり直すようにしたものである。もちろん、条件としてこれ以外にも、電源電圧が低下した場合や、認証情報記憶装置 9 が分離されなくても利用者の手が触れた場合などが考えられる。

【0041】さらに、本実施例では認証情報記憶装置 9 の読み書きは同時に一つの認証情報で許可されるようにしたが、例えば認証情報記憶装置 9 の読取りと、書き込みを異なる認証情報で出来るようにすれば、ホスト装置を管理している管理者が、まず書き込み用の認証情報で必要な第二認証情報を記憶し、その後この認証情報記憶装置 9 を利用者に配布することによって、利用者に対してホスト装置への接続を制限する一方で、利用者毎に一個の第二認証情報だけでホスト装置（複数も含む）を管理出来ない場合でも、利用者は読み出し用の第一認証情報だけを覚えるだけで戸惑うことなくホスト装置を利用できる。もちろん、読み出し用の第一認証情報はその利用者のみが知っているものなので、セキュリティも保つことが出来る。

【0042】なお、本実施例では特に図示しないが、認証情報記憶装置 9 へ第二認証情報 9 2 を記憶させる手順は、読み出しと同様にまず第一認証情報 9 1 を入力して、次いで検索条件 9 3 とこれに対応する第二認証情報 9 2 を書き込むことで行えるが、既に記憶しているレコードに書き込もうとした検索条件 9 3 と完全に一致する検索条件がある場合には、第二認証情報の更新をする旨を利用者 1 0 に通知する。さらに、認証情報記憶装置 9 に記憶できる空き領域が不足した場合には、新しい認証情報記憶装置 9 を用意することを利用者 1 0 に促すが、

新しい認証情報記憶装置 9 に交換したときには、始めに第一認証情報の設定を行い、その後第二認証情報を書き込むことになる。

【0043】また図 8 は図 5 のデータ構造において、各レコード毎に第二認証情報 9 2 に関する属性情報 9 6 を付加した例で、属性情報 9 6 には例えば各第二認証情報の使用回数や、何に関するホスト装置であるか、あるいはその認証情報をいつ取得したか、さらにその第二認証情報 9 2 の有効期限などを記録しておくことで、認証情報の削除や更新などのメンテナンスに利用することが出来る。

【0044】なお、以上に説明した本実施例に利用できる認証情報記憶装置の形状や接続方式は、分離型で携帯性を重視するような場合には、例えば ISO 7816 に準拠した IC カードが挙げられる。

【0045】また端末装置に内蔵するような場合は、同じく ISO 7816 に準拠する機能をもった IC チップを実装するか、またはこのような機能を端末装置を制御する CPU と一緒に一つの IC チップに収めるなどが考えられる。

【0046】〔第二実施例〕図 9 は、本発明の第二実施例に係わる情報システムの概念図である。本実施例は、認証情報を記憶する装置として、記憶したデータの読み書きに関して何ら保護する機能を持たないものを使用した場合の例である。ただし、第一実施例と同様に複数の第二認証情報 9 2 を記憶し、利用者 10 はこれらを一個の情報を覚えるだけで必要に応じてホスト装置へ送信することが出来るようにしている点は同じである。また、同図において、先の実施例と均等なものには同一番号を付し、その説明は重複を避ける為に省略する。

【0047】図 9 において、13 は端末装置 8 をホスト装置に接続するために要求される情報を記憶するが、データの読み書きは認証情報などの制約無しにいつでも行えるデータ記憶装置である。

【0048】14 はデータ記憶装置 13 に記憶する第二認証情報 9 2 を後述する暗証情報 16 によって暗号化して暗号第二認証情報 9 7 を出力する第二認証情報暗号化処理、15 は第二認証情報暗号化処理 14 とは逆に、暗証情報 16 で暗号第二認証情報 9 7 を復号化して元の第二認証情報 9 2 を出力する第二認証情報復号化処理、16 は利用者 10 が暗記している情報で、第二認証情報暗号化処理 14 および第二認証情報復号化処理 15 において第二認証情報 9 2 を暗号化および復号化する際の鍵情報となる暗証情報である。9 7 は第二認証情報暗号化処理 14 で暗証情報 16 によって暗号化された第二認証情報で、データ記憶装置 13 に記憶されている暗号第二認証情報である。

【0049】図 10 は本実施例において、ホスト装置 A 1 より文書 “pubindex.htm” を端末装置 8 に取り寄せるときの流れを示した図であり、処理は S 1 から S 10 へ

と進む。

【0050】本実施例の動作を図 9 および図 10 を用いて説明する。

【0051】ここでは、第一実施例と同様にホスト装置 A 1 に目的の情報があり、ホスト装置 A 1 はインターネット 4 に接続されており、目的の情報は URL 8 2 で指定し、さらに指定された情報は第二認証情報が要求されるとする。

【0052】まず、利用者 10 は図 10 に示すように、まず端末装置 8 を起動 (S 1) し、データ記憶装置 13 を端末装置 8 に接続する (S 2)。

【0053】次に、利用者 10 は図 9 にあるようにブラウザソフト 12 を使って、端末装置 8 を公衆回線 7 から公衆回線網 6 を通じてインターネットプロバイダ 5 に接続し、URL 8 2 を指定してホスト装置 A 1 に接続を行い (S 3)、そして目的の文書名 “pubindex.htm” をパケット 11 に乗せてホスト装置 A 1 へ送信 (S 4)。ホスト装置 A 1 は文書 “pubindex.htm” に認証確認が設定されていると、この事を端末装置 8 へ通知し、利用者 10 に対して第二認証情報 9 2 の送信を要求する。こゝまでは第一実施例と同様である。

【0054】次に、第二認証情報 9 2 の送信を要求された端末装置 8 のブラウザソフト 12 はこの要求を検出 (S 5) すると、URL 8 2 から検索条件 9 3 を取り出し、データ記憶装置 13 から検索条件 9 3 を用いて暗号第二認証情報 9 7 を読み出す (S 6)。

【0055】読み出された暗号第二認証情報 9 7 は暗号化された状態なので、復号化の必要がある。そこでブラウザソフト 12 は利用者 10 に暗証情報 16 の入力を要求する (S 7)。

【0056】暗証情報 16 を入力されると、ブラウザソフト 12 はこれを第二認証情報復号化処理 15 に暗号第二認証情報 9 7 と共に入力し、復号化し第二認証情報 9 2 を得る。

【0057】ブラウザソフト 12 はこのようにして第二認証情報 9 2 を受け取ると、第一実施例と同様に図 4 に示した利用者 ID 入力欄 8 3 と、認証情報入力欄 8 4 からホスト装置 A 1 に対して第二認証情報 9 2 を送信し、これが確認 (S 9) されると、文書 “pubindex.htm” が送信され、ブラウザソフト 12 はこれを順次受信して、端末装置 8 の画面に文書を表示する (S 10)。

【0058】以降、利用者 10 が新たな URL 8 2 を入力し、第二認証情報 9 2 が要求される度に、図 10 に示す S 4 から S 10 の処理を繰り返すが、暗証情報 16 は一度入力したので、S 7 はスキップされる。

【0059】このように処理が行われることにより利用者 10 は、一度だけ暗証情報 16 を入力しておけば、特定のホスト装置あるいは特定の文書毎に第二認証情報を要求されるような場合、さらにはそのような認証情報の内容がばらばらであるような場合でも、必要とされる第

二認証情報が予めデータ記憶装置 13 に記憶してあれば、自動的に第二認証情報 9 2 が送信されるので、複数の認証情報をまとめて一個の暗証情報を覚えておくだけで利用できるもので非常に使い勝手が良い。

【0060】また、認証情報は利用者以外に漏れることがないようにしなければならないが、本実施例ではデータ記憶装置 13 に記憶されたデータは暗号化されているので、たとえ端末装置 8 から分離して紛失したような場合でも、第二認証情報 9 2 が他人に漏れる心配が無い。もちろん、データ記憶装置 13 が端末装置 8 と一体になっているような場合でもこれらの利点が失われることがないのは明白である。

【0061】なお、以上のように構成することで、第一実施例で説明した第二認証情報を自動的に読み出せる有効期限の制御や、検索条件に該当するものがないときの処理、同じ検索条件での第二認証情報は更新処理を実行、属性情報の付加、データ記憶装置が端末装置に接続されていないときの処理、検索条件を構成するデータの種類などは第一実施例と同等のものを本実施例でも実現できる。

【0062】また、本実施例のようにデータ記憶装置自身には記憶した情報を保護する機能がなく、そのため記憶するデータ自身を暗号化するなどして漏洩を防止した場合、端末装置の仕様またはブラウザソフトの機能が同じであれば、データ記憶装置を単体で持ち歩き、他の端末装置からでもホスト装置を利用できるが、データ記憶装置内のデータ記録フォーマットの違いや、暗号化／復号化処理の有無あるいは相違があると、利用できない。

【0063】そこでこれらへの対応には、例えば記録フォーマットでは、同じデータを複数の形式のフォーマットで記憶することで改善できる。また、暗号化や復号化の処理はこれらの処理を行うプログラムをその端末のアーキテクチャに合わせて作り、これまた複数の形式のフォーマットで記憶しておくことで改善を図れる。

【0064】

【発明の効果】本発明によれば、利用者は情報をホスト装置から取寄せる時に、複数の認証情報をホスト装置に

送信する必要がある場合でも、利用者は唯一、一個の認証情報を入力するだけで、その後はホスト装置または情報への認証処理が簡単に行えるようになる。

【図面の簡単な説明】

【図 1】第一実施例の情報システムの概念図である。

【図 2】第一実施例および第二実施例を説明するためのホスト装置に登録されている利用者 ID などの例を示す図である。

【図 3】第一実施例および第二実施例を説明するための画面表示の例を示す図である。

【図 4】第一実施例および第二実施例を説明するための画面表示の例を示す図である。

【図 5】第一実施例のデータ構造を説明する図である。

【図 6】第一実施例の処理の流れを示す説明図である。

【図 7】第一実施例で認証情報を自動的に取り出せる期間の制御を説明するフロー図である。

【図 8】第一実施例のデータ構造の説明を補足する図である。

【図 9】第二実施例である情報システムの概念図である。

【図 10】第二実施例の処理の流れを示す説明図である。

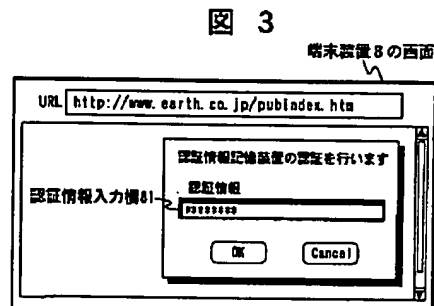
【符号の説明】

1…ホスト装置 A、 2…ホスト装置 B、 3…ホスト装置 C、 4…インターネット、 5…インターネットプロバイダ、 6…公衆回線網、 7…公衆回線、 8…端末装置、 8 1…認証情報入力欄、 8 2…Uniform Resource Locator (URL)、 8 3…利用者 ID 入力欄、 8 4…認証情報入力欄、 9…認証情報記憶装置、 9 1…第一認証情報、 9 2…第二認証情報、 9 3…検索条件、 9 4…利用者 ID、 9 5…認証情報、 9 6…属性情報、 9 7…暗号第二認証情報、 10…利用者、 11…バケット、 12…ブラウザソフト、 13…データ記憶装置、 14…第二認証情報暗号化処理、 15…第二認証情報復号化処理、 16…暗証情報。

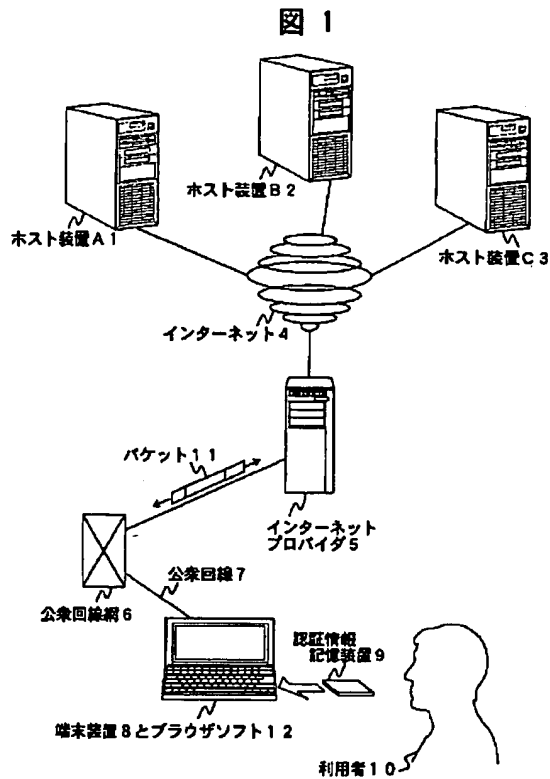
【図 2】

図 2			
ホスト装置	利用者 ID	認証情報	サーバ名
A	IslandABC	173161n54	//www.earth.co.jp
B	Jungle123	4Au5Eg6Ca	//www.peace.co.jp
C	CanyonXYZ	4Au5Eg6Ca	//www.space.co.jp

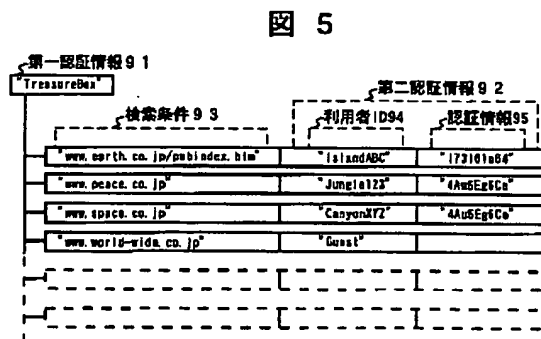
【図 3】



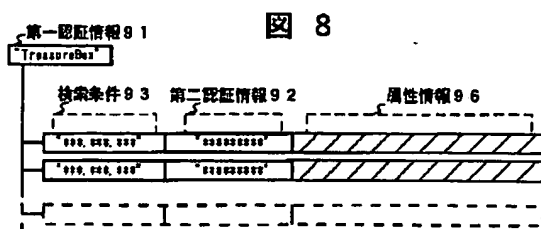
【図 1】



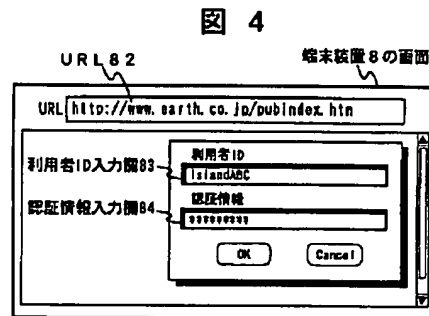
【図 5】



【図 8】

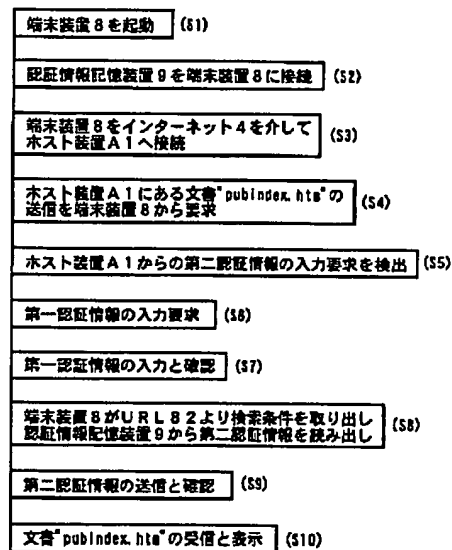


【図 4】



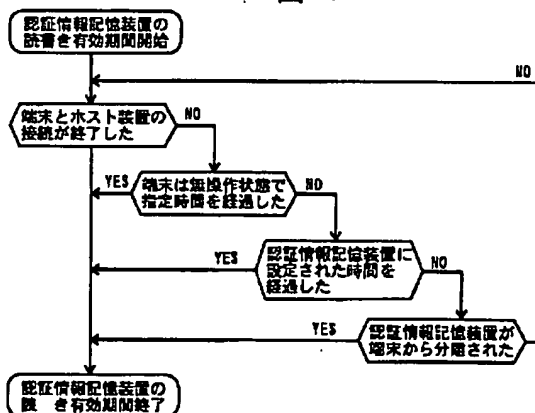
【図 6】

図 6



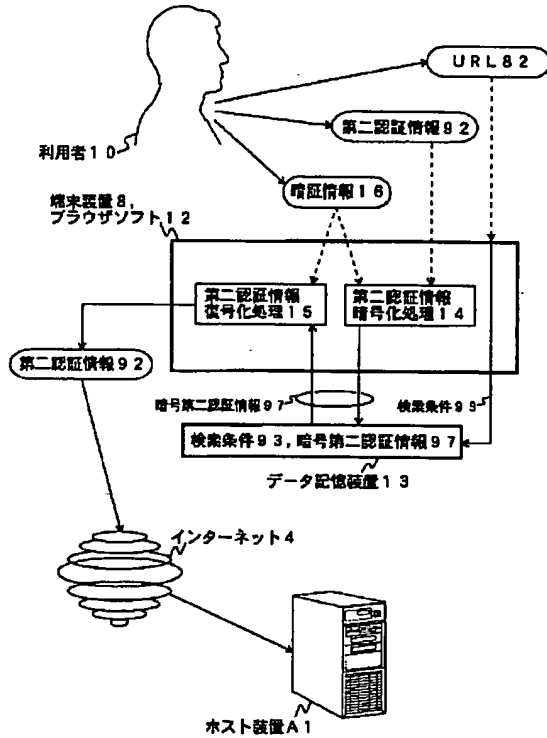
【図 7】

図 7



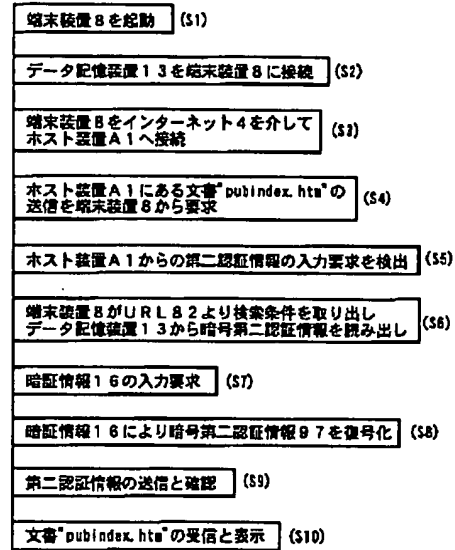
【図 9】

図 9



【図 10】

図 10



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-025051

(43)Date of publication of application : 29.01.1999

(51)Int.Cl.

G06F 15/00

G06F 1/00

(21)Application number : 09-183433

(71)Applicant : HITACHI LTD

(22)Date of filing : 09.07.1997

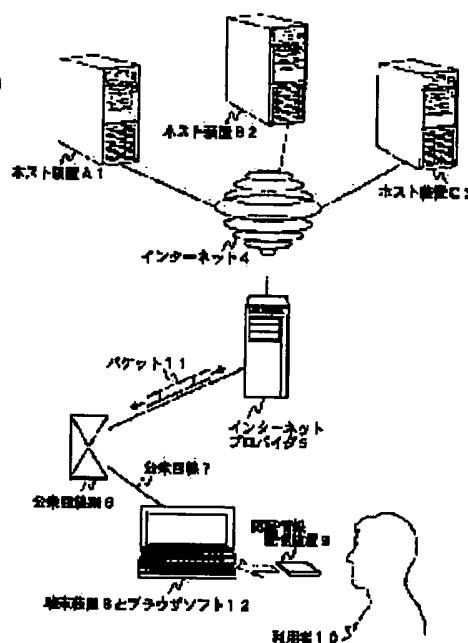
(72)Inventor : YOKOZAWA TATSU
ADACHI MAKOTO

(54) INFORMATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To improve operability by allowing a user to input only one certification information for easily operating a certification processing for a host device or the information afterwards.

SOLUTION: A certification information storage device 9 stores second certification information requested for connecting a terminal equipment 8 with a host device, and first certification information for protecting the second certification information from being leaked to the others. Host devices A1, B2, and C3 corresponding to a word wide web(WWW) connected with an internet 4 request the second certification information for confirming that a user 10 is a legal user at the time of connection with the terminal equipment 8. The user 10 inputs the first certification information only once so that the second certification information can be automatically transmitted when the second certification information is requested for each specific host device or specific document as long as the necessary second certification information is preliminarily stored in the certification information storage device 9.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the
examiner's decision of rejection or application
converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of
rejection][Date of requesting appeal against examiner's decision
of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

Prior Art Document 2

[Claim 1]

An information system comprising: a host device and a terminal device;

said host device in which various items of information are stored and said items of information are retrievable by a user with said terminal device, said host device having a function for requesting a user authentication information for confirming that the user is an authorized registrant at the time of the retrieval of said items of information by the user; and

said terminal device, which is capable of transmitting/receiving data by connecting to the host device, having a function for retrieving said various items of information and presenting the information to a user, and a function for receiving an input by a user, said information system further comprising:

an authentication information storage device which stores various kinds of data, the data are being readable/writable by said terminal device, and has a function for storing first authentication information for authorizing reading/writing the data before the data are actually read/written, and a function for performing authorization processing; wherein

said authentication information storage device stores authentication information which is required in said host device as second authentication information, and said authentication information storage device or said terminal device has a function for reading/writing the second authentication information selectively, whereby

even in the case where a plurality of kinds of second authentication information are required, a user does not need necessarily to remember respective authentication information but need to remember said first authentication information, thereby enabling the user to read out necessary second authentication information by easy selection to complete confirmation operation necessary for establishing a connection to said host device.

[Claim 2]

The information system according to claim 1, wherein:

said host device and said terminal device have a function for transmitting/receiving information by protocol, respectively; and

Prior Art Document 2

said terminal device has a function for detecting, by the protocol, whether or not confirmation operation is necessary for connecting to said host device, a function for reading out said second authentication information from said authentication information storage device and transmitting it to said host device in response to the success of detection and a function for performing the confirmation operation in advance with regard to said authentication information storage device using said first authentication information; whereby

a user does not need necessarily to input said first authentication information, every time the user is requested, by said host device, to input said second authentication information.

[0014]

Fig. 2 shows examples of "user ID", its corresponding "authentication information" required to obtain information from a host device A1, a host device B2, and a host device C3, and "server name" indicating the respective host device.

【Fig. 2】

HOST DEVICE	USER ID	AUTHENTICATION INFORMATION	SERVER NAME
A	IslandABC	173161n64	//www.earth.co.jp
B	Jungle123	4Au6Eg6Ce	//www.peace.co.jp
C	CanyonXYZ	4Au6Eg6Ce	//www.space.co.jp